REMARKS

The Examiner has rejected Claims 1-32 and 34 under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent No. 5,968,176) and further in view of Reid et al. (U.S. Patent No. 6,182,226) in view of Vaidya (U.S. Patent No. 6,279,113). Applicant respectfully disagrees with such rejection.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

With respect to the first element of the prima facie case of obviousness and, in particular, the obviousness of combining the aforementioned references, the Examiner argues that a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett by employing a firewall capable of virus scanning, as in Reid. The Examiner also argues that a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Nessett by scanning for signature files, as in Vaidya. To the contrary, applicant respectfully asserts that it would not have been obvious to combine the teachings of the Nessett, Reid and Vaidya references, especially in view of the vast evidence to the contrary.

For example, Nessett relates to a **Network Interface Card (NIC)** firewall, while Reid and Vaidya relate to **external** firewalls. To simply glean features from an NIC firewall, such as that of Nessett, and combine the same with the *non-analogous art* of

external firewalls, such as that of Reid and Vaidya would simply be improper. External firewalls protect multiple computers, while a NIC firewall protects the computer to which it is attached. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems an NIC firewall addresses as opposed to an external firewall, the Examiner's proposed combination is in appropriate.

In addition, contrary to the Examiner's arguments, applicant's claimed feature would have been unobvious in view of Reid and Vaidya, since Reid and Vaidya's external firewalls *teach away* from any sort of processor positioned on a network adapter coupled between a computer and a network. In addition, they also *teach away* from such a processor that is adapted for virus scanning and content scanning of network traffic transmitted between the computer and the network, in the manner claimed by applicant. *In re Hedges*, 783 F.2d 1038, 228 USPQ 685 (Fed. Cir. 1986).

More importantly, with respect to the third element of the prima facie case of obviousness, applicant respectfully asserts that the prior art references, when combined, fail to teach or suggest all of the claim limitations.

With respect to the independent claims, the Examiner has relied on Col. 11, lines 26-31 in Nessett and Col. 8, lines 10-18 in Reid, as excerpted below, to make a prior art showing of applicant's claimed technique "wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the computer and the network" (see this or similar, but not identical language in each of independent Claims 1, 14, 27 and 29) and "logic positioned on a network adapter means for virus scanning and content scanning of the packets" (see Claim 28).

"The use of filtering for security purposes can occur in NICs, Switches, Repeaters, Routers, and Remote Access Equipment. Filtering within a NIC can be used to ensure the source MAC addresses it sends are valid and that the source addresses it receives are from trusted end systems. However, NIC filtering can be used for other equally valid purposes, such as offloading VLAN enforcement processing from Hubs, implementing pervasive multilayer firewalls, and providing hardware support for higher level security protocols." (Nessett-Col. 11, lines 51-62)

"The firewall's access control diagrams also include the capability of sending alerts, with an administrator-defined message, based on any connection decision. Alerts can be dropped into the access flow diagrams at any point. If a connection reaches that point in the diagram, the alert is triggered. For example, in FIG. 4, a check for viruses is performed on a file (70). If a virus is found, the administrator is alerted (72), and the transfer is redirected to a safe location for later inspection (74)." (Reid-Col. 8, lines 10-18)

First, applicant notes that the above cited excerpts relied on by the Examiner merely teach filtering within an NIC "to ensure the source MAC addresses it sends are valid and that the source addresses it receives are from trusted end systems." However, applicant respectfully asserts that filtering, as in Nessett, does not meet content scanning, as claimed by applicant, especially since the only filtering done in Nessett relates to source addresses. The Examiner has argued that a firewall, which may include the filtering of Nessett (see Col. 11, line 61), must implicitly scan packets to determine if they are blocked or allowed. Applicant respectfully disagrees. Content of a packet does not necessarily have to be scanned in the Examiner's hypothetical firewall since, for example, a source or destination address (not the content) are the filtering criteria used in such a firewall.

Applicant further emphasizes that, for example, virus scanning, by definition, involves a utility that searches for viruses, and optionally removes any that are found. Such functionality is simply not met by Nessett's firewall that solely prevents unauthorized access. Since network adapters are often ingress points for many untrusted files and data that may proliferate on an associated computer, virus and content scanning of network traffic on a processor positioned on a network adapter creates an enhanced layer of security at the network adapter.

Second, applicant notes that Reid only teaches that the firewall includes the capability of sending alerts based on a virus check. Clearly, Reid does not teach that the firewall performs the virus check, but only that the firewall performs the alert based on a virus check. In fact, Reid teaches access control rules on the firewall (see Col. 7, lines 33-59), none of which include performing virus scanning. Thus, neither the Nessett reference nor the Reid reference teach "a processor positioned on a network adapter...[that] is adapted for virus scanning," in the manner claimed by applicant.

Also with respect to each of the independent claims, the Examiner has relied on Col. 3, lines 12-26 in Vaidya to make a prior art showing of applicant's claimed technique "wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data."

> "The dynamic signature-based network IDS includes multiple attack signature profiles which are each descriptive of identifiable characteristics associated with particular network intrusion attempts associated with network objects located on the network. Network intrusion attempts include unauthorized attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction of a network object. The attack signature profiles can include generic attack and/or customized attack signature profiles for particular network objects on the network. Customized attack signature profiles can be added to a set of generic attack signature profiles without having to modify the processor, thereby facilitating efficient customization of the IDS." (Col. 3, lines 12-26-emphasis added)

Applicant notes that the above cited excerpt from Vaidya relied on by the Examiner merely teaches general "attack signature profiles" which are "associated with particular network intrusion attempts." Applicant asserts that signatures for intrusion attempts do not rise to the level of specificity of applicant's claimed "virus signatures," especially in view of the list of intrusion attempts included in Vaidya, namely "attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction of a network object."

Again, with respect to the third element of the prima facie case of obviousness, applicant respectfully asserts that the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

The Examiner's rejections are also deficient with respect to the dependent claims, since such rejections also do not meet each and every element of the prima facie case. For example, with respect to dependent Claim 6 et al., the Examiner has relied on Col. 7, lines 9-21 in Nessett to make a prior art showing of applicant's claimed technique "wherein the manner in which the scanning is performed is capable of being user-configured." Applicant respectfully asserts that such excerpt merely discloses filtering rules. Clearly filtering rules does not meet applicant's specific claim language, namely "the manner in which the scanning is performed" (emphasis added) since filtering rules only identify types of data that may be allowed access.

With respect to Claim 10 et al., the Examiner has relied on Col. 23, lines 18-26 in Nessett to make a prior art showing of applicant's claimed technique "wherein the processor is capable of passing received packets that are not of interest to the computer." Applicant notes, however, that such excerpt gives an example where "end systems...would not be able to receive any traffic other than FTP requests" since any traffic other than FTP requests would not be of interest. However, this example *teaches away* from applicant's claim language, since applicant claims that "the processor is capable of passing received packets that are not of interest to the computer" (emphasis added).

With respect to Claim 11 et al., the Examiner has relied on Col. 23, lines 18-26 in Nessestt to make a prior art showing of applicant's claimed technique "wherein the processor is capable of scanning received packets that are of interest." The Examiner further states that scanning is implied from the ability to distinguish between the different protocols. Applicant asserts that it seems the Examiner has failed to consider the full

weight of applicant's claim language. Applicant claims "scanning received packets that are of interest," (emphasis added), and not simply scanning received packets to determine if they are of interest, as in Nessett.

With respect to Claim 30, the Examiner has relied on Col. 17, lines 9-21 in Nessett to make a prior art showing of applicant's claimed technique "wherein the content scanning enforces operational policies of an organization." Applicant respectfully asserts that such excerpt only generally teaches managing security policy data. Clearly, managing security policy data for the operation of security systems, as in Nessett, does not meet any sort of content scanning, and especially not content scanning that "enforces operational policies in an organization," as specifically claimed by applicant.

With respect to Claim 31, the Examiner has relied on Col. 3, lines 12-26 in Vaidya to make a prior art showing of applicant's claimed technique "wherein the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation." Applicant asserts that such excerpt merely teaches network intrusion attempts, such as "unauthorized attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction of a network object," none of which meet any of applicant's specifically claimed policies.

With respect to Claim 32, the Examiner has simply dismissed applicant's claimed technique "wherein the virus signature files are stored on a non-volatile solid state memory on the network adapter" as being obvious. Applicant respectfully asserts that since none of the references relied on by the Examiner teach virus scanning on a network adapter in the context claimed by applicant (see independent Claim 1), it would not have been obvious to store signature files "on a non-volatile solid state memory on the network adapter," as further claimed by applicant.

With respect to Claim 34, the Examiner has relied on Col. 11, lines 35-47 in Vaidya to make a prior art showing of applicant's claimed technique "wherein the received packets that are of interest include executable files." Applicant asserts that such excerpt merely teaches executing an expression instruction from an expression instruction list, and not that received packets that are of interest are executable files, in the manner claimed by applicant.

Again, a notice of allowance or a specific prior art showing of each of such claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P056/01.187.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100